



Industrial Control Systems Cyber Security Advanced Training

The United States Department of Homeland Security Control Systems Security Program in coordination with the Australian Attorney-General's Department is pleased to announce the Industrial Control Systems Cyber Security Advanced Training for Australia.

This event will provide intensive hands-on training on protecting and securing control systems from cyber attacks, including a Red Team/Blue Team exercise that will be conducted within an actual control systems environment. It will also provide an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

Where and When? The Control Systems Analysis Center located in Idaho Falls, Idaho, USA, TBD 2009.

Who Should Attend? Developers, IT/process control security personnel, network engineers and managers who are responsible for operation and oversight of critical infrastructure.

Prerequisites: Each attendee should have practical knowledge with respect to networks, software and control system

components; have basic coding skills and a fairly deep understanding of network details such as the difference between UDP and TCP, as well as MAC and IP addresses. **Every student attending this course must bring a laptop computer** (with DVD drive) that they can configure.

Registration: This event is limited to approximately 35 people. All registrations will be vetted and verified through the Australian Government Attorney-General's Department and the Idaho National Laboratory Security Plan requirements.

Structure and Agenda: This event includes four full days of intensive control systems security training and presentations with a 12-hour Red Team/Blue Team exercise:

- Day 1** — Welcome and introductions, hands-on classroom training on current cyber security techniques and practices.
- Day 2** — Continue hands-on classroom training on current cyber security techniques and practices, training on defensive techniques for control systems and separation into the Red Team and the Blue Team.
- Day 3** — Break-out sessions will be provided to help students with topics they would like more information on, and tools they would like more experience with, such as Network Discovery and Mapping, Intrusion Detection, Network Exploration, and Metasploit.
- Day 4** — Red Team/Blue Team exercise (12 hour exercise) where participants will be tasked with either attacking (Red Team) or defending (Blue Team) a small chemical batch mixing plant.
- Day 5** — Exercise debrief and roundtable discussion.

